Week 3- Securing Cloud Storage

Name- Samruddhi Dattu Nikam

PRN- 2124UCSF2019

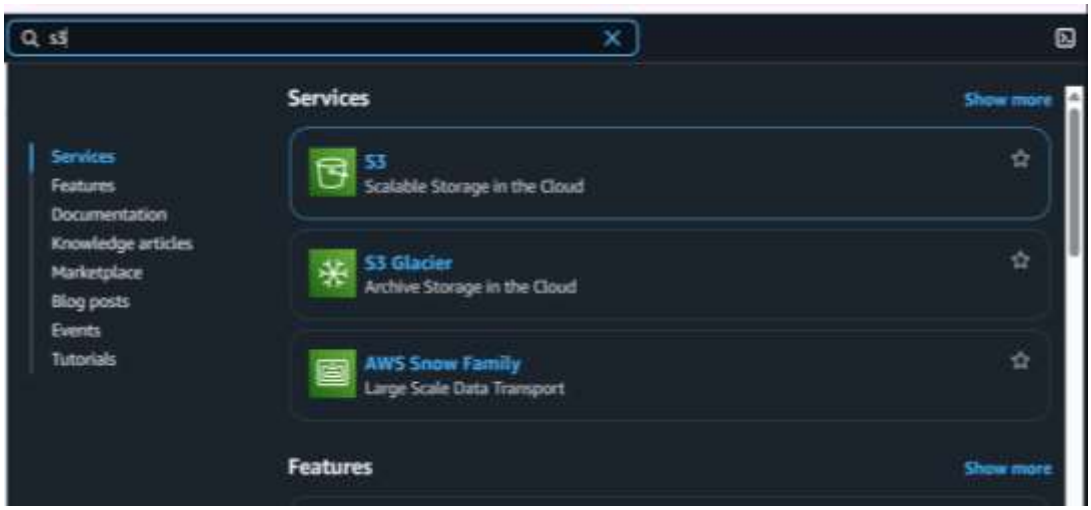
Email Id- samruddhi.nikam_24ucs@sanjivani.edu.in

College Name- Sanjivani University

❖ **Task-** 1) Set up S3 bucket .
2) Apply access control policies.
3) Document security configurations.

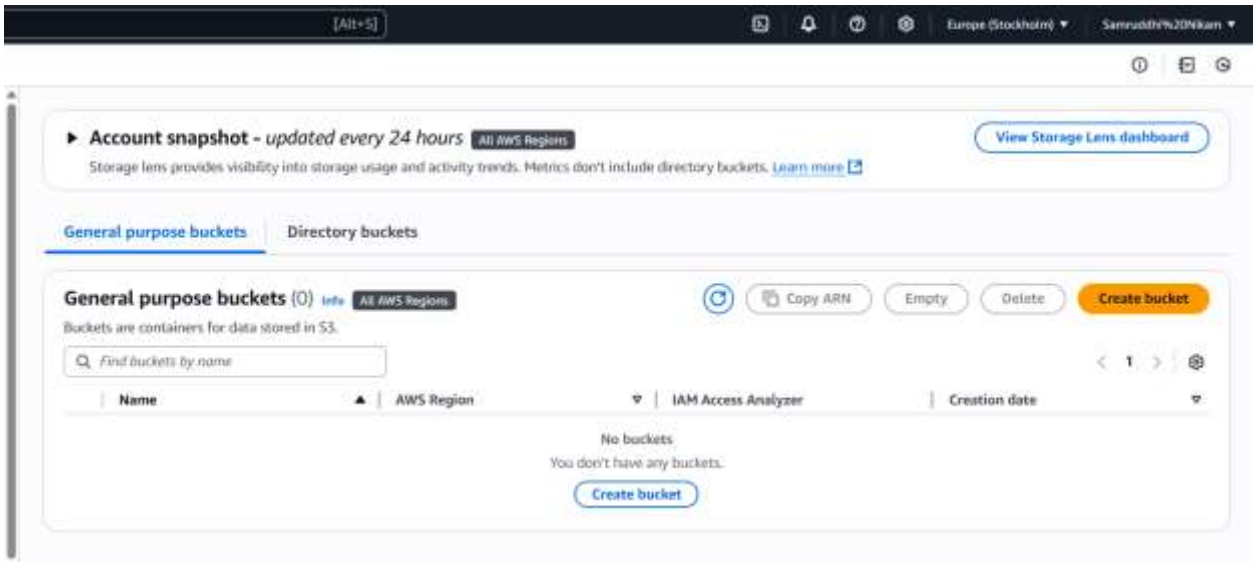
Step Set up S3 Bucket.

1. Logged in to AWS Console**.**
2. Search S3 and then click.

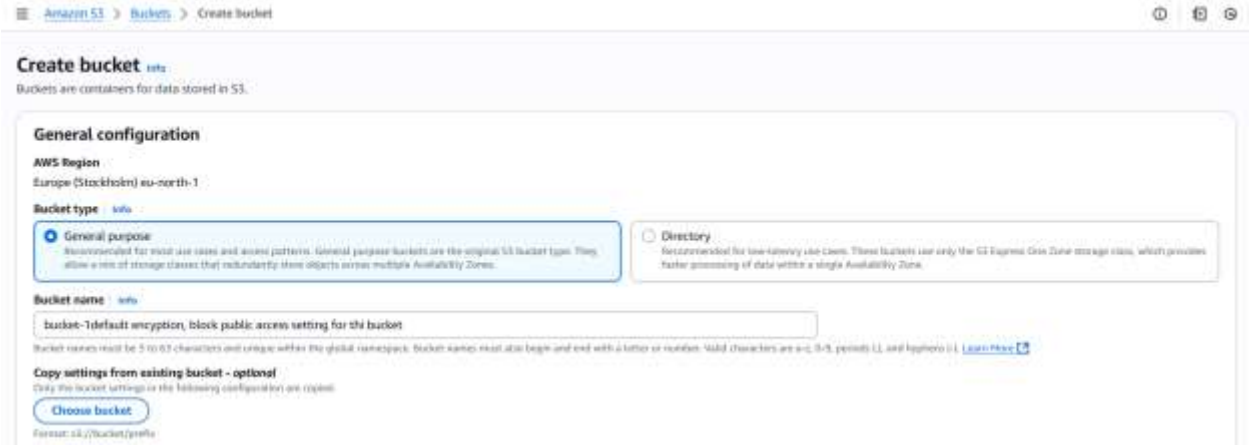


3. Then Click Create bucket Option.

Week 3- Securing Cloud Storage



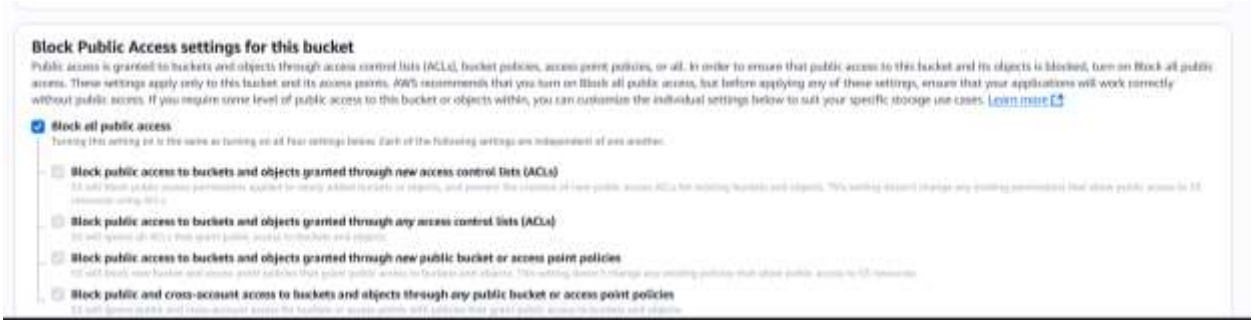
4. Enter the Bucket name and select the Bucket type.



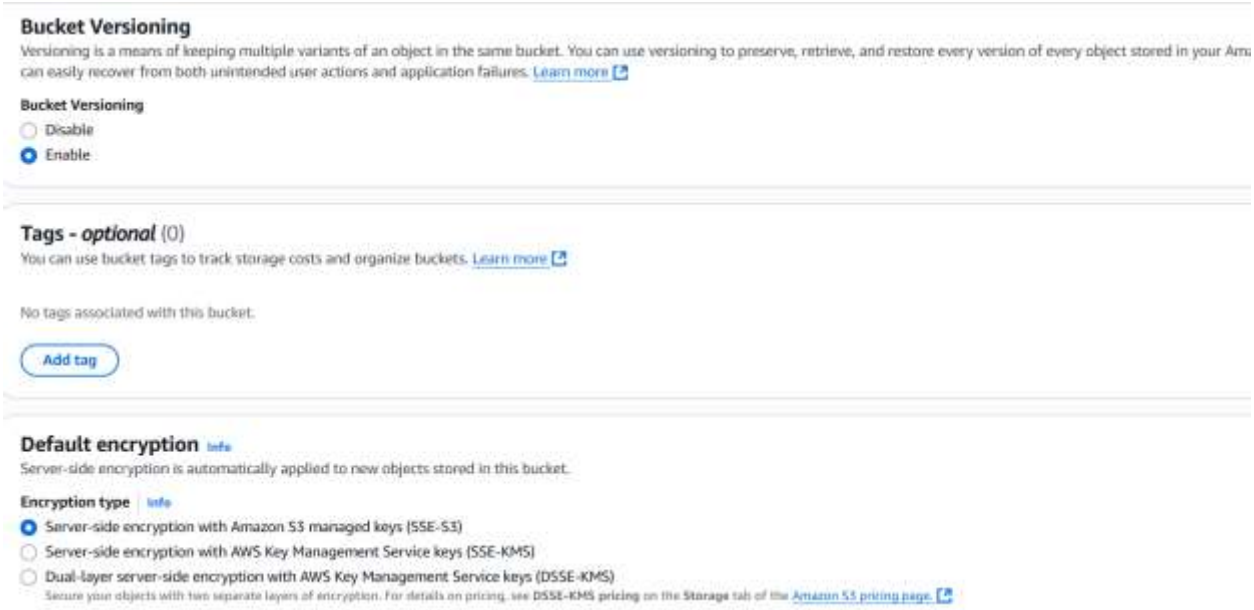
5. Select the Object Ownership

Week 3- Securing Cloud Storage

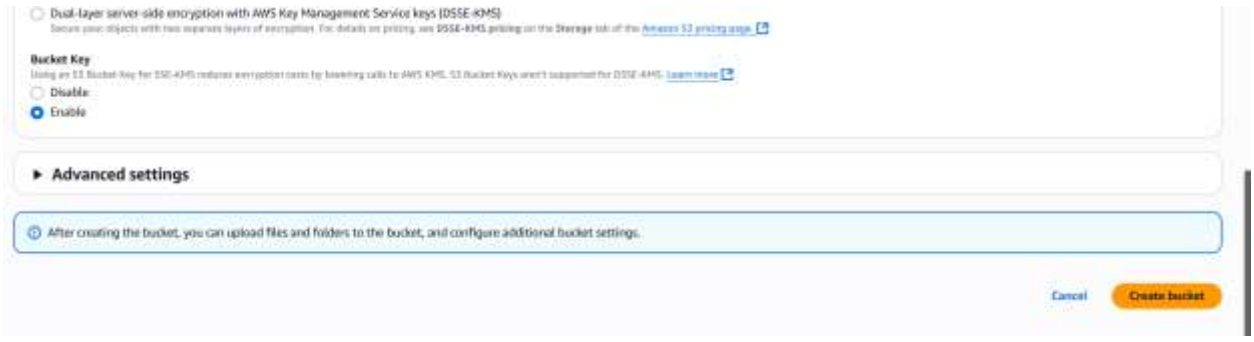
6. Block Public access Setting for this bucket.



7. Select Bucket versioning Enable, and then select Default encryption server-side encryption with amazon S3managed keys(SSE-S3).

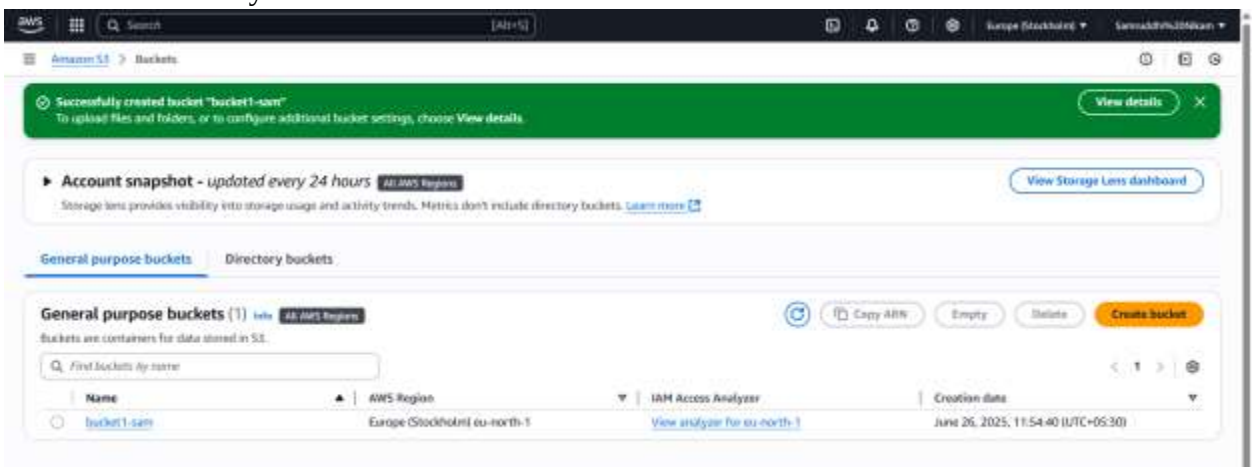


8. Select Bucket key Enable, and then click create bucket button.



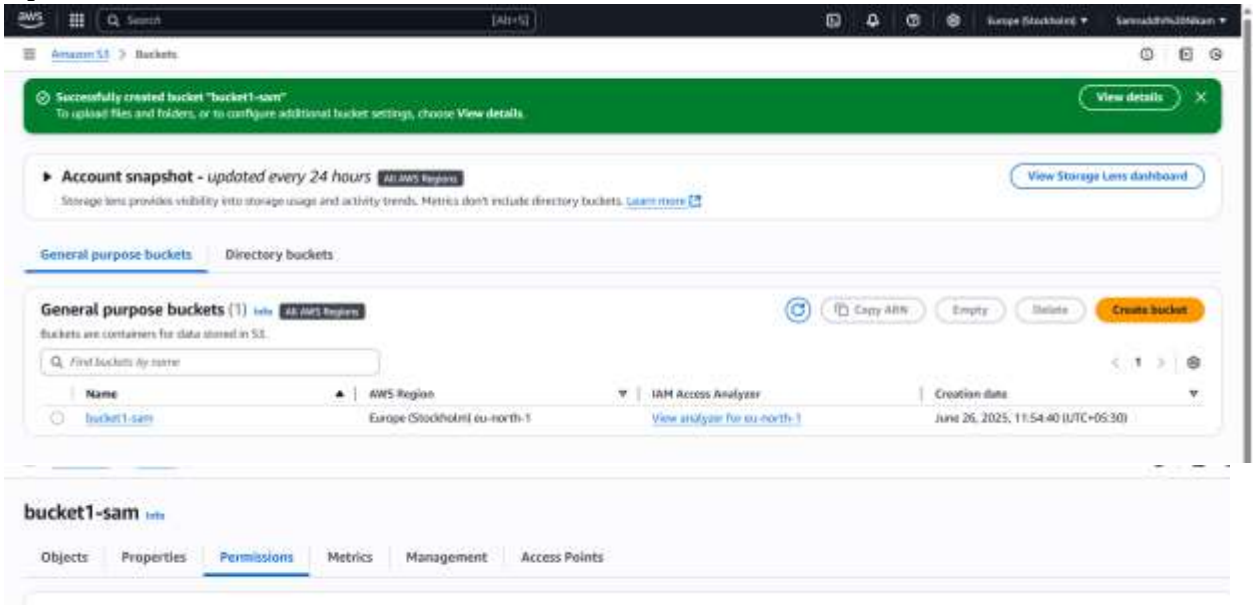
Week 3- Securing Cloud Storage

9. Bucket Successfully Created.



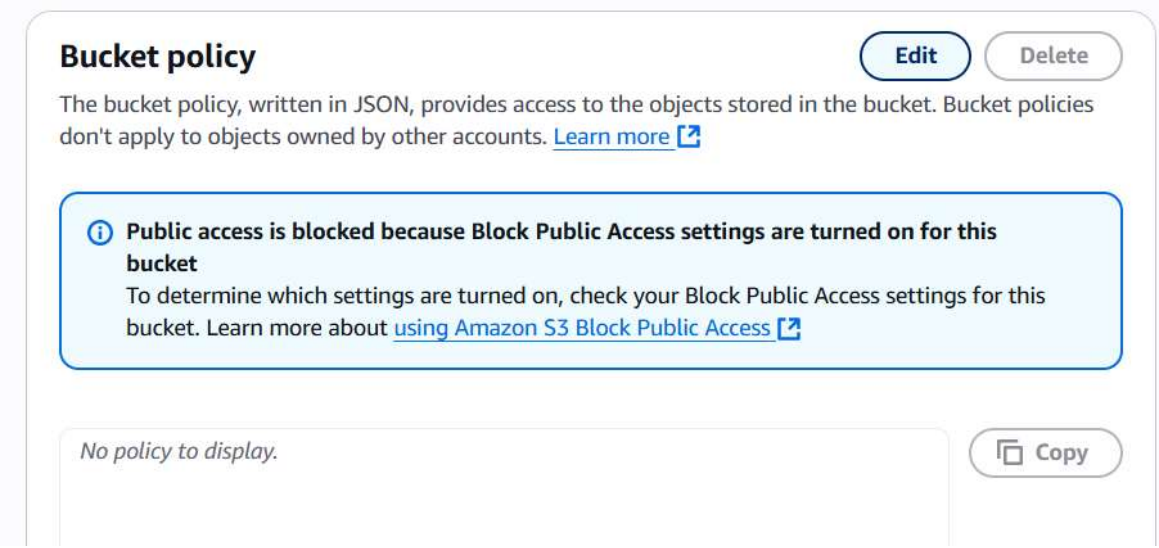
Steps Apply Access control Policies.

1. Open S3 >Bucket > bucket1-sam> Permission.



2. Scroll- down and Click Edit.

Week 3- Securing Cloud Storage



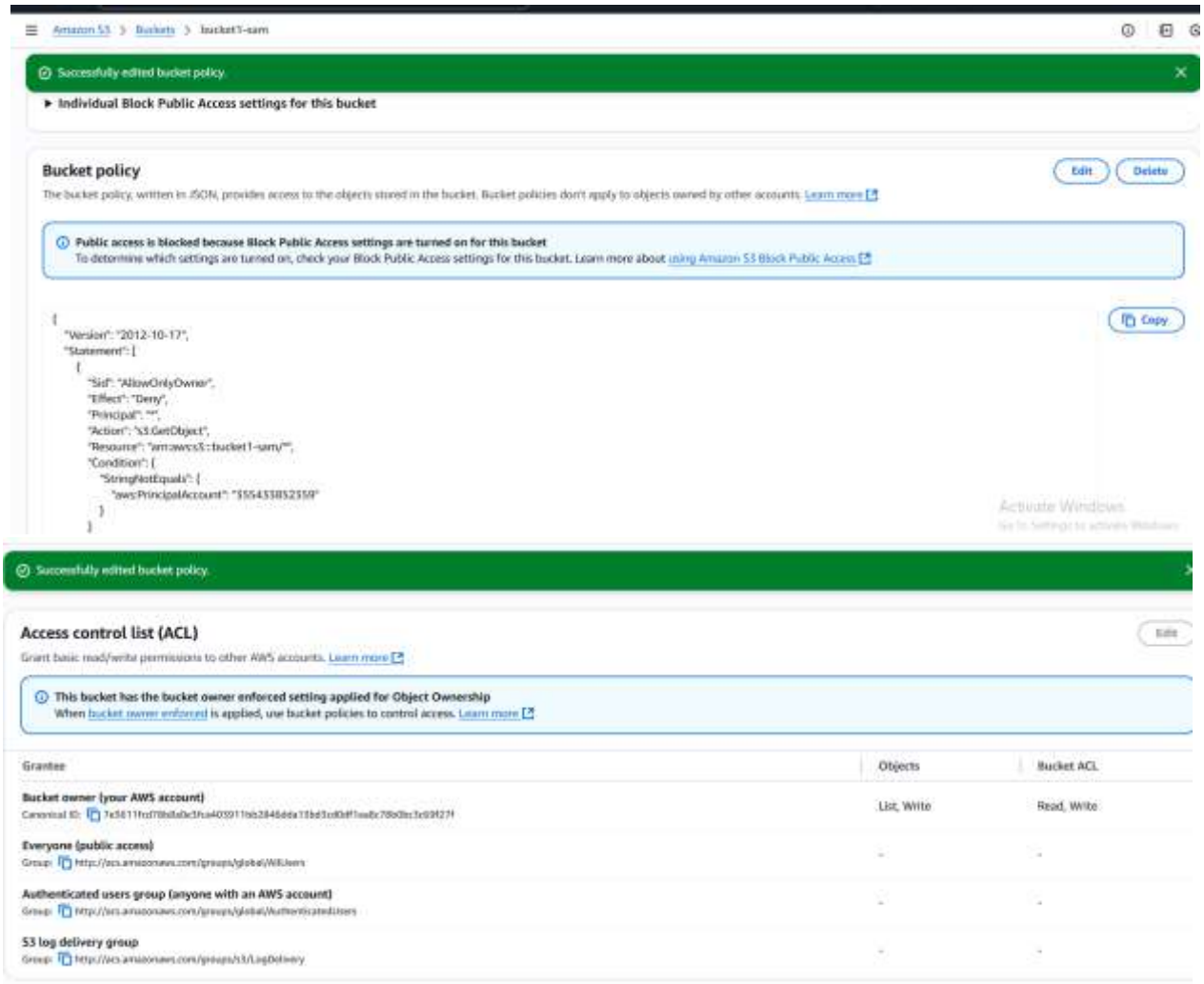
3. Then Write then write the following code to block public access, and save the policy.

Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowOnlyOwner",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::bucket1-sam/*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "355433852359"
        }
      }
    }
  ]
}
```

4. Save the policy → Now only the bucket owner's account can access the objects. All other access is denied.

Week 3- Securing Cloud Storage

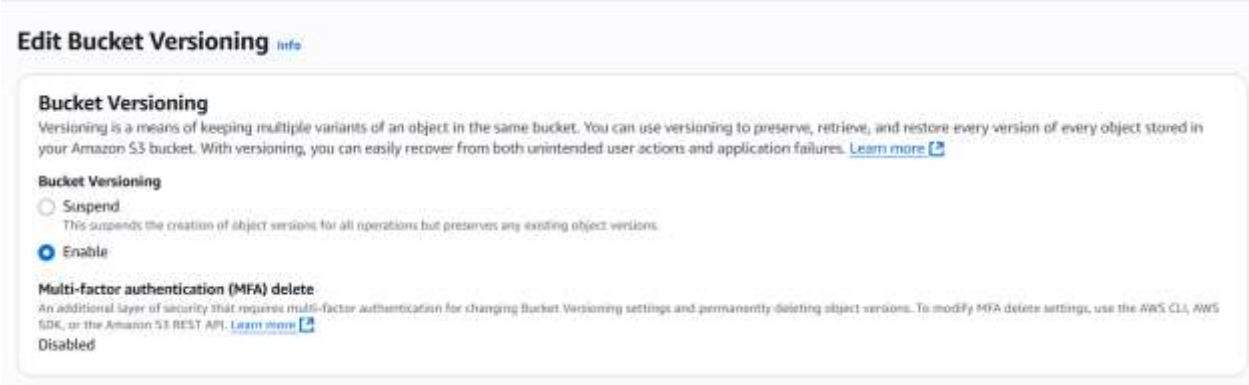


Task 3- Document security configurations.

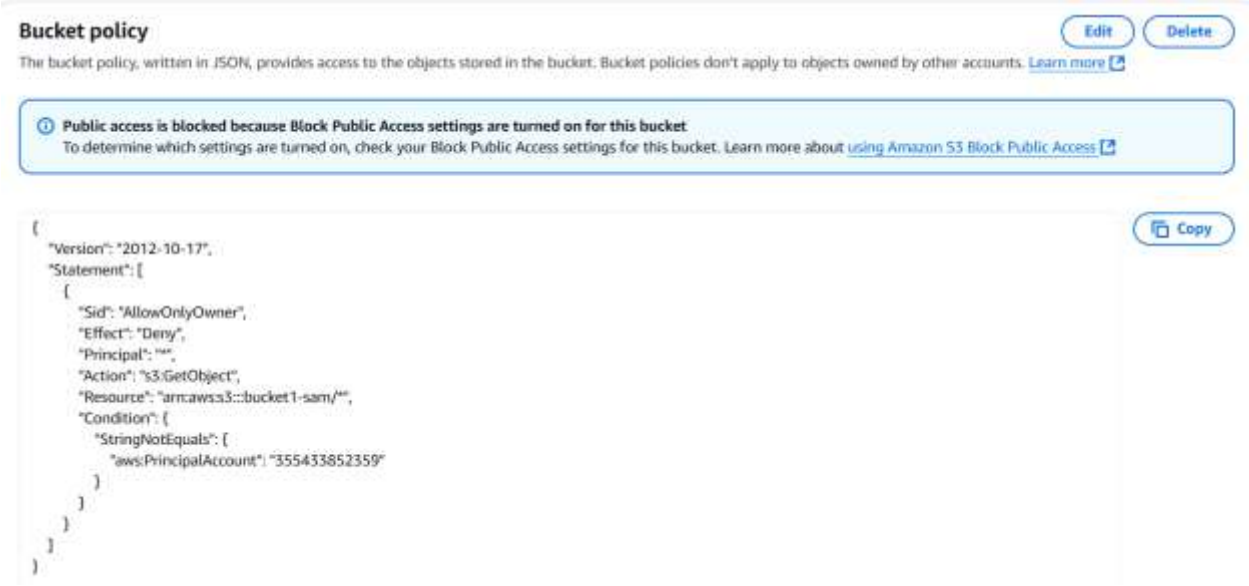
- Default encryption with Amazon S3 managed keys (SSE-S3) is enabled to protect all objects by default.

Week 3- Securing Cloud Storage

- Versioning is enabled to keep all versions of objects for recovery and rollback



- Access policy restricts object access to only the bucket owner's account



- Public access is blocked using AWS's Block Public Access settings for added security.